UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/786,030	02/26/2004	Ahmed E. Hassan	42783-0040	2914

23577	7590	12/12/2007

RIDOUT & MAYBEE
SUITE 2400
ONE QUEEN STREET EAST
TORONTO, ON M5C3B1
CANADA

EXAMINER
ADDY, ANTHONY S

ART UNIT	PAPER NUMBER
2617	

MAIL DATE	DELIVERY MODE
12/12/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

	Application No.	Applicant(s)
Office Action Summary	10/786,030	HASSAN ET AL.
	Examiner	Art Unit
	Anthony S. Addy	2617

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>01 October 2007</u>.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>15,19-24,26 and 29-34</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>15, 19-24, 26 and 29-34</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a) ☐ All b) ☐ Some * c) ☐ None of:

       1. ☐ Certified copies of the priority documents have been received.

       2. ☐ Certified copies of the priority documents have been received in Application No. _____.

       3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1.   This action is in response to applicant's amendment filed on October 1, 2007.

Claim 25 has been cancelled and new **claims 29-34** has been added. **Claims 15, 19-**

24, 26 and **29-34** are currently pending in the present application.

Response to Arguments

2.   Applicant's arguments with respect to **claims 15, 19-24, 26** and **29-34** have been

considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

3.   The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that

form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

4.   Claims 32-34 are rejected under 35 U.S.C. 102(a) as being anticipated by

Tuulos, WO 03/081932 A1 (hereinafter Tuulos).

Regarding claim 32, Tuulos discloses a method for providing security to a mobile

electronic device having a device lock module that restricts use of the mobile electronic

device by a user thereof by locking the device under predetermined circumstances (see

abstract, page 11, lines 9-20 and p. 14, lines 4-7), the method comprising: receiving

input signals from an input device of the mobile electronic device (see page 6, lines 22-

25 and page 14, lines 4-7); determining if the mobile electronic device is in a secure

location based on the input signals (see page 6, lines 15-20, page 13, lines 1-13 and

Fig. 4; *shows a GPS receiver 40 for determining location information for the mobile device based on input signals received*); requiring input of a first predetermined password by a user to unlock the mobile electronic device if it is in the secure location (see page 11, lines 18-20 [*i.e. the teaching of Tuulos, that the when the MS 23 is operating in a second security mode (safe area), the MS 23 requires a shorter password or less frequent PIN equates to the claimed limitations of "requiring input of a first predetermined password by a user to unlock the mobile electronic device if it is in the secure location"*]) and requiring input of a second predetermined password by a user to unlock the mobile electronic device if it is not in the secure location (see page 11, lines 9-18 [*i.e. the teaching of Tuulos, that the when the MS 23 is operating in a first security mode (unsafe area), the MS 23 requires a longer password or PIN equates to the claimed limitations of "requiring input of a second predetermined password by a user to unlock the mobile electronic device if it is not in the secure location"*]).

Regarding claim 33, Tuulos discloses all the limitations of claim 32. In addition, Tuulos discloses a method, applying if the mobile device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile device will be locked if user interaction with the mobile device is not detected (see page 11, lines 9-20 [*i.e. Tuulos inherently teaches the claimed limitations of "applying if the mobile device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile device will be locked if user interaction with the mobile device is not detected," since Tuulos teaches if the mobile device (MS 23) is determined to be in a secure location (i.e. during the second security mode the MS 23*

determines that it is in a relatively safe area), a shorter less complex password is

*required or **requires less frequent PIN or password access** which inherently shows*

that if the mobile device is determined to be in a secure location a longer countdown

timer is required since Tuulos teaches the mobile device requires less frequent PIN or

password access in a secure location]), and applying, if the mobile device is determined

not to be in a secure location, a second, shorter, countdown timer value defining the

duration after which the mobile device will be locked if user interaction with the mobile

device is not detected (see page 11, lines 9-20 [*i.e. Tuulos inherently teaches the*

claimed limitations of "applying, if the mobile device is determined not to be in a secure

location, a second, shorter, countdown timer value defining the duration after which the

mobile device will be locked if user interaction with the mobile device is not detected,"

since Tuulos teaches if the mobile device (MS 23) is determined not to be in a secure

location (i.e. during the first security mode the MS 23 determines that it is in a relatively

*unsafe area), a longer more complex password is required or it might **be necessary to***

***input a PIN or password each time the phone is accessed** which inherently shows*

that if the mobile device is determined not to be in a secure location a shorter

countdown timer is required since Tuulos teaches it might be necessary to input a PIN

or password each time the phone is accessed when the mobile device is determined not

to be in a secure location compared to when the mobile device is in a secure location

which requires a longer countdown timer since less frequent PIN or password access is

required]).

Regarding claim 34, Tuulos discloses all the limitations of claim 32. In addition, Tuulos discloses a method, wherein the second predetermined password required to unlock the mobile device if it is not in a secure location is more complex than the first predetermined password required to unlock the mobile device if it is in a secure location (see *Tuulos*, page 11, lines 9-20).

Claim Rejections - 35 USC § 103

5.   The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6.   Claims 15, 19, 22, 23, 26, 29, 30 and 31 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Fogle et al., U.S. Publication Number 2003/0074590 A1 (hereinafter Fogle)**, and further in view of **Tuulos, WO 03/081932 A1 (hereinafter Tuulos)**.

Regarding claim 15, Fogle teaches a mobile device (*e.g. PDAs/laptop*) (see p. 1 [0015] and Fig.1), comprising: a processor (see p. 1 [0015] and Fig.1); at least a first input device connected to the processor for providing input signals thereto (see p. 2 [0018-0020] and Fig.1); and an output device connected to the processor for providing output to a user of the mobile device (see p. 2 [0018-0019] and Fig.1); and a device lock module associated with the processor for implementing a lock mode (*e.g. standby/lock utility 44*) which places restrictions on user access to the mobile device if user input activity for the mobile device falls below a threshold (see p. 3 [0030-0036], p. 3 [0040-0044], p. 5 [0060] and Fig. 1; shows an electronic device 10 including a standby/lock

utility 44 [i.e. the standby/lock utility 44 reads on a lock module, since the electronic
device 10 uses the standby/lock utility 44 to automatically activate a lock mode when
there is no user action or input such as pressing a key on the keyboard 28]).

Fogle fails to explicitly teach the processor being configured for determining
location information for the mobile device based on input signals received from the first
input; and the device lock module being configured for determining if the mobile device
is in a secure location based on the determined location information, and requiring input
of a first predetermined password by a user to unlock the mobile device if it is in a
secure location and requiring input of a second predetermined password by a user to
unlock the mobile device if it is not in a secure location.

In an analogous field of endeavor, Tuulos teaches a method and apparatus for
implementing at least first and second security levels in a mobile telecommunications
device for use within a telecommunications network, wherein a location of the mobile
device is determined, and one of the first and second security levels is selected on the
basis of that location (see abstract). According to Tuulos, a processor (*e.g. GPS
receiver 40*) is configured for determining location information for the mobile device
based on input signals received from a first input (see page 6, lines 15-20, page 13,
lines 1-13 and Fig. 4; *shows a GPS receiver 40 which reads on a processor configured
for determining location information for the mobile device based on input signals
received from a first input*); and the device lock module being configured for determining
if the mobile device is in a secure location based on the determined location
information, and requiring input of a first predetermined password by a user to unlock

the mobile device if it is in a secure location and requiring input of a second

predetermined password by a user to unlock the mobile device if it is not in a secure

location (see page 11, lines 9-20).

It would therefore have been obvious to one of ordinary skill in the art at the time

of the invention to modify Fogle with Tuulos to include a mobile device, wherein the

processor being configured for determining location information for the mobile device

based on input signals received from the first input; and the device lock module being

configured for determining if the mobile device is in a secure location based on the

determined location information, and requiring input of a first predetermined password

by a user to unlock the mobile device if it is in a secure location and requiring input of a

second predetermined password by a user to unlock the mobile device if it is not in a

secure location, in order to apply different security levels to a mobile telecommunication

device based on whether the current location of the mobile telecommunication device is

determined to be at a safe or unsafe location as taught by Tuulos (see abstract and

page 11, lines 9-20).

Regarding claim 19, Fogle in view of Tuulos teaches all the limitations of claim

15. Fogle in view of Tuulos further teaches a mobile device, wherein the device lock

module is configured for determining the threshold in dependence on the determined

location information (see Tuulos, page 11, lines 9-20).

Regarding claim 22, Fogle in view of Tuulos teaches all the limitations of claim

15. Fogle in view of Tuulos further teaches a mobile device, wherein the first input

device includes a GPS receiver (see *Tuulos,* page 6, lines 15-20, page 13, lines 4-6 and

Fig. 4; *shows a GPS receiver 40).*

Regarding claim 23, Fogle in view of Tuulos teaches all the limitations of claim

15. Fogle in view of Tuulos further teaches a mobile device, wherein the first input

device includes a wireless communications subsystem connected to the processor for

exchanging communications signals with a wireless network including a plurality of base

stations, the location information being determined based on identities of the base

stations (see *Tuulos,* page 6, lines 1-20 and page 9, lines 19-22).

Regarding claim 26, Fogle teaches a method for providing security to a mobile

electronic device (*e.g. PDAs/laptop*) (see p. 1 [0015] and Fig.1) having a device lock

module (*e.g. standby/lock utility 44*) that restricts use of the mobile electronic device by

a user thereof by locking the electronic device when user interaction with the mobile

device falls below a threshold (see p. 3 [0030-0036], p. 3 [0040-0044], p. 5 [0060] and

Fig. 1; shows an electronic device 10 including a standby/lock utility 44 [i.e. the

standby/lock utility 44 reads on a device lock module, since the electronic device 10

uses the standby/lock utility 44 to automatically activate a lock mode when there is no

user action or input such as pressing a key on the keyboard 28), the method

comprising: receiving input signals from an input device of the mobile electronic device

(see p. 2 [0018-0020] and Fig.1).

Fogle fails to explicitly teach determining if the mobile electronic device is in a

secure location based on the input signals; and applying, if the mobile electronic device

is determined to be in a secure location, a first countdown timer value defining a

duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected, and applying, if the mobile electronic device is determined not to be in a secure location, a second, shorter, countdown timer value defining the duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected.

In an analogous field of endeavor, Tuulos teaches a method and apparatus for implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network, wherein a location of the mobile device is determined, and one of the first and second security levels is selected on the basis of that location (see abstract). According to Tuulos, a processor (*e.g. GPS receiver 40*) is configured for determining location information for the mobile device based on input signals received from a first input (see page 6, lines 15-20, page 13, lines 1-13 and Fig. 4; *shows a GPS receiver 40 which reads on a processor configured for determining location information for the mobile device based on input signals received from a first input*); and the device lock module being configured for determining if the mobile device is in a secure location based on the determined location information, and requiring input of a first predetermined password by a user to unlock the mobile device if it is in a secure location and requiring input of a second predetermined password by a user to unlock the mobile device if it is not in a secure location (see page 11, lines 9-20). In addition, Tuulos teaches, applying if the mobile device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile device will be locked if user interaction with the mobile

device is not detected (see page 11, lines 9-20 [*i.e. Tuulos inherently teaches the*

claimed limitations of "applying if the mobile device is determined to be in a secure

location, a first countdown timer value defining a duration after which the mobile device

will be locked if user interaction with the mobile device is not detected," since Tuulos

teaches if the mobile device (MS 23) is determined to be in a secure location (i.e. during

the second security mode the MS 23 determines that it is in a relatively safe area), a

*shorter less complex password is required or **requires less frequent PIN or password***

***access** which inherently shows that if the mobile device is determined to be in a secure*

location a longer countdown timer is required since Tuulos teaches the mobile device

requires less frequent PIN or password access in a secure location]), and applying, if

the mobile device is determined not to be in a secure location, a second, shorter,

countdown timer value defining the duration after which the mobile device will be locked

if user interaction with the mobile device is not detected (see page 11, lines 9-20 [*i.e.*

Tuulos inherently teaches the claimed limitations of "applying, if the mobile device is

determined not to be in a secure location, a second, shorter, countdown timer value

defining the duration after which the mobile device will be locked if user interaction with

the mobile device is not detected," since Tuulos teaches if the mobile device (MS 23) is

determined not to be in a secure location (i.e. during the first security mode the MS 23

determines that it is in a relatively unsafe area), a longer more complex password is

*required or it might **be necessary to input a PIN or password each time the phone is***

***accessed** which inherently shows that if the mobile device is determined not to be in a*

secure location a shorter countdown timer is required since Tuulos teaches it might be

necessary to input a PIN or password each time the phone is accessed when the mobile device is determined not to be in a secure location compared to when the mobile device is in a secure location which requires a longer countdown timer since less frequent PIN or password access is required]).

It would therefore have been obvious to one of ordinary skill in the art at the time of the invention to modify Fogle with Tuulos to include a method of determining if the mobile electronic device is in a secure location based on the input signals; and applying, if the mobile electronic device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected, and applying, if the mobile electronic device is determined not to be in a secure location, a second, shorter, countdown timer value defining the duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected, in order to apply different security levels to a mobile telecommunication device based on whether the current location of the mobile telecommunication device is determined to be at a safe or unsafe location as taught by Tuulos (see abstract and page 11, lines 9-20).

Regarding claim 29, Fogle in view of Tuulos teaches all the limitations of claim 15. Fogle in view of Tuulos further teaches a mobile device, wherein the device lock module is configured to apply, if the mobile device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile device will be locked if user interaction with the mobile device is not detected (see page 11, lines 9-20 [*i.e. Tuulos inherently teaches the claimed limitations of " apply, if the mobile*

device is determined to be in a secure location, a first countdown timer value defining a

duration after which the mobile device will be locked if user interaction with the mobile

device is not detected," since Tuulos teaches if the mobile device (MS 23) is determined

to be in a secure location (i.e. during the second security mode the MS 23 determines

that it is in a relatively safe area), a shorter less complex password is required or

requires less frequent PIN or password access *which inherently shows that if the*

mobile device is determined to be in a secure location a longer countdown timer is

required since, Tuulos teaches the mobile device requires less frequent PIN or

password access in a secure location]), and apply, if the mobile device is determined

not to be in a secure location, a second, shorter, countdown timer value defining the

duration after which the mobile device will be locked if user interaction with the mobile

device is not detected (see page 11, lines 9-20 [i.e. Tuulos inherently teaches the

claimed limitations of "apply, if the mobile device is determined not to be in a secure

location, a second, shorter, countdown timer value defining the duration after which the

mobile device will be locked if user interaction with the mobile device is not detected,"

since Tuulos teaches if the mobile device (MS 23) is determined not to be in a secure

location (i.e. during the first security mode the MS 23 determines that it is in a relatively

unsafe area), a longer more complex password is required or it might ***be necessary to***

input a PIN or password each time the phone is accessed *which inherently shows*

that if the mobile device is determined not to be in a secure location a shorter

countdown timer is required since, Tuulos teaches it might be necessary to input a PIN

or password each time the phone is accessed when the mobile device is determined not

to be in a secure location compared to when the mobile device is in a secure location which requires a longer countdown timer since less frequent PIN or password access is required]).

Regarding claim 30, Fogle in view of Tuulos teaches all the limitations of claim 15. Fogle in view of Tuulos further teaches a mobile device, wherein the second predetermined password required to unlock the mobile device if it is not in a secure location is more complex than the first predetermined password required to unlock the mobile device if it is in a secure location (see *Tuulos*, page 11, lines 9-20).

Regarding claim 31, Fogle teaches a mobile device (*e.g. PDAs/laptop*) (see p. 1 [0015] and Fig.1), comprising: a processor (see p. 1 [0015] and Fig.1); at least a first input device connected to the processor for providing input signals thereto (see p. 2 [0018-0020] and Fig.1); at least one user input device connected to the processor and having a physical user interface responsive to user input activity (see p. 2 [0018-0020] and Fig.1); an output device connected to the processor for providing output to a user of the mobile device (see p. 2 [0018-0019] and Fig.1); and a device lock module associated with the processor for implementing a lock mode (*e.g. standby/lock utility 44*) which places restrictions on user access to the mobile device if user input activity for the mobile device falls below a threshold (see p. 3 [0030-0036], p. 3 [0040-0044], p. 5 [0060] and Fig. 1; shows an electronic device 10 including a standby/lock utility 44 [i.e. the standby/lock utility 44 reads on a lock module, since the electronic device 10 uses the standby/lock utility 44 to automatically activate a lock mode when there is no user action or input such as pressing a key on the keyboard 28]).

Fogle fails to explicitly teach the processor being configured for determining location information for the mobile device based on input signals received from the first input; and the device lock module being configured for determining if the mobile device is in a secure location based on the determined location information and to apply, if the mobile electronic device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected, and apply, if the mobile electronic device is determined not to be in a secure location, a second, shorter, countdown timer value defining the duration after which the mobile electronic device will be locked if user interaction with the mobile electronic device is not detected.

In an analogous field of endeavor, Tuulos teaches a method and apparatus for implementing at least first and second security levels in a mobile telecommunications device for use within a telecommunications network, wherein a location of the mobile device is determined, and one of the first and second security levels is selected on the basis of that location (see abstract). According to Tuulos, a processor (*e.g. GPS receiver 40*) is configured for determining location information for the mobile device based on input signals received from a first input (see page 6, lines 15-20, page 13, lines 1-13 and Fig. 4; *shows a GPS receiver 40 which reads on a processor configured for determining location information for the mobile device based on input signals received from a first input*); and the device lock module being configured for determining if the mobile device is in a secure location based on the determined location information, and requiring input of a first predetermined password by a user to unlock

the mobile device if it is in a secure location and requiring input of a second predetermined password by a user to unlock the mobile device if it is not in a secure location (see page 11, lines 9-20). In addition, Tuulos teaches, applying if the mobile device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile device will be locked if user interaction with the mobile device is not detected (see page 11, lines 9-20 [*i.e. Tuulos inherently teaches the claimed limitations of "applying if the mobile device is determined to be in a secure location, a first countdown timer value defining a duration after which the mobile device will be locked if user interaction with the mobile device is not detected," since Tuulos teaches if the mobile device (MS 23) is determined to be in a secure location (i.e. during the second security mode the MS 23 determines that it is in a relatively safe area), a shorter less complex password is required or **requires less frequent PIN or password access** which inherently shows that if the mobile device is determined to be in a secure location a longer countdown timer is required since Tuulos teaches the mobile device requires less frequent PIN or password access in a secure location*]), and applying, if the mobile device is determined not to be in a secure location, a second, shorter, countdown timer value defining the duration after which the mobile device will be locked if user interaction with the mobile device is not detected (see page 11, lines 9-20 [*i.e. Tuulos inherently teaches the claimed limitations of "applying, if the mobile device is determined not to be in a secure location, a second, shorter, countdown timer value defining the duration after which the mobile device will be locked if user interaction with the mobile device is not detected," since Tuulos teaches if the mobile device (MS 23) is*

determined not to be in a secure location (i.e. during the first security mode the MS 23

determines that it is in a relatively unsafe area), a longer more complex password is

*required or it might **be necessary to input a PIN or password each time the phone is***

***accessed** which inherently shows that if the mobile device is determined not to be in a*

secure location a shorter countdown timer is required since Tuulos teaches it might be

necessary to input a PIN or password each time the phone is accessed when the

mobile device is determined not to be in a secure location compared to when the mobile

device is in a secure location which requires a longer countdown timer since less

frequent PIN or password access is required]).

It would therefore have been obvious to one of ordinary skill in the art at the time

of the invention to modify Fogle with Tuulos to include a mobile device, comprising: the

processor being configured for determining location information for the mobile device

based on input signals received from the first input; and the device lock module being

configured for determining if the mobile device is in a secure location based on the

determined location information and to apply, if the mobile electronic device is

determined to be in a secure location, a first countdown timer value defining a duration

after which the mobile electronic device will be locked if user interaction with the mobile

electronic device is not detected, and apply, if the mobile electronic device is

determined not to be in a secure location, a second, shorter, countdown timer value

defining the duration after which the mobile electronic device will be locked if user

interaction with the mobile electronic device is not detected, in order to apply different

security levels to a mobile telecommunication device based on whether the current

location of the mobile telecommunication device is determined to be at a safe or unsafe

location as taught by Tuulos (see abstract and page 11, lines 9-20).

7.   Claims 20 and 21 are rejected under 35 U.S.C. 103(a) as being unpatentable

over **Fogle et al., U.S. Publication Number 2003/0074590 A1 (hereinafter Fogle)** and

Tuulos, WO 03/081932 A1 (hereinafter Tuulos) as applied to claim 15 above, and

further in view of **Landram et al., U.S. Publication Number 2005/0077997 A1**

(hereinafter Landram).

Regarding claims 20 and 21, Fogle in view of Tuulos teaches all the limitations of

claim 15. Fogle in view of Tuulos fails to explicitly teach a mobile device, wherein the

first input device includes an interface for docking the mobile device to a desktop

computer, the location information being determined based on whether the mobile

device is docked to the desktop computer and wherein the security setting of the device

lock module is set to mirror that of the desktop computer when the mobile device is

docked to the desktop computer.

Landram, however, teaches a mobile terminal allocation system, wherein a

cradle provides a docking interface for a respective mobile terminal to communicate

with a host computer through a wireless link or via a network connection through the

cradle (see p. 2 [0025] and Fig. 1). Landram further teaches the location information of

the mobile terminal is determined based on whether the mobile device is docked to the

desktop computer and wherein the security setting of the device lock module is set to

mirror that of the desktop computer when the mobile device is docked to the desktop

computer (see p. 2 [0028-0030] and p. 4 [0067-0069]).

It would therefore have been obvious to one of ordinary skill in the art at the time

of the invention to modify Fogle and Tuulos with Landram to include a mobile device,

wherein the first input device includes an interface for docking the mobile device to a

desktop computer, the location information being determined based on whether the

mobile device is docked to the desktop computer and wherein the security setting of the

device lock module is set to mirror that of the desktop computer when the mobile device

is docked to the desktop computer, in order to securely store mobile devices allocated

to different users and based on authentication results, allow a host computer

communicating with the mobile devices through a docking interface to automatically

select a mobile device for a user as taught by Landram (see p. 2 [0026]).

8.   Claim 24 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Fogle et**

al., U.S. Publication Number 2003/0074590 A1 (hereinafter Fogle) and **Tuulos, WO**

03/081932 A1 (hereinafter Tuulos) as applied to claim 15 above, and further in view of

Huang, U.S. Publication Number 2005/0164720 A1 (hereinafter Huang).

Regarding claim 24, Fogle in view of Tuulos teaches all the limitations of claim

15. Fogle in view of Tuulos further teaches the mobile device is enabled for receiving

electronic messages (see *Fogle*, p. 2 [0021]), but fails to explicitly teach the mobile

device includes a message filtering module associated with the processor for filtering

electronic messages received by the mobile device, the message filtering module being

configured for changing filtering criteria for filtering the electronic messages in

dependence on the determined location information.

Huang, however, teaches a method of filtering messages received on a receiving

telephone apparatus, wherein filtering rules are applied to a received message at the

telephone apparatus and if the message satisfies at least one of the filtering rules, a

filtering process is then executed on the message (see p. 1 [0007], p. 1 [0014] and

Figures 3 & 4).

It would therefore have been obvious to one of ordinary skill in the art at the time

of the invention to modify Fogle and Tuulos with Huang to include a message filtering

module associated with the processor for filtering electronic messages received by the

mobile device, in order to automatically filter out unwanted messages according to the

filtering rules and prevent the user of the telephone apparatus to manually filter out

unwanted messages as taught by Huang (see p. 1 [0008]).

Conclusion

9.   Applicant's amendment necessitated the new ground(s) of rejection presented in

this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP

§ 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37

CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE

MONTHS from the mailing date of this action. In the event a first reply is filed within

TWO MONTHS of the mailing date of this final action and the advisory action is not

mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

10.   Any inquiry concerning this communication or earlier communications from the examiner should be directed to Anthony S. Addy whose telephone number is 571-272-7795. The examiner can normally be reached on Mon-Thur 8:00am-6:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Duc M. Nguyen can be reached on 571-272-7503. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

A.S.A

DUC M. NGUYEN
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2600